INTRODUCING CYBER SECURITY ASSUMPTION BUSTER WORKSHOPS

There is a strong and often repeated call for research to provide novel cyber security solutions. The rhetoric of this call is that our new solutions be radically different from existing solutions; making incremental improvements is a losing proposition; we are lagging behind and need technological leaps to get, and keep, ahead of adversaries who are themselves rapidly improving attack technology. To answer this call, we must examine the key assumptions that underlie current security architectures. Challenging those assumptions both opens up the possibilities for novel solutions that are rooted in a fundamentally different understanding of the problem and provides even stronger basis for moving forward on those assumptions that are well-founded.

The Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group is conducting a series of four workshops to begin the assumption buster process. The assumptions that underlie this series is that cyber space is an adversarial domain, that the adversary is stubborn and clever, and that re-examining our cyber security architectures with these assumptions in mind will result in key insights that will lead to the novel solutions we desperately need. To assure that our discussion has the requisite adversarial flavor, we are inviting researchers that develop solutions in of the type under discussion, and researchers that exploit these solutions. The aim is to have robust debate of topics long held to be true to determine to what extent that claim is warranted. The adversarial nature of these debates will assure the threat environment is reflected in the discussion and the research concepts that result from these workshops will have a greater chance of having a sustained positive impact on our cyber security posture.

The four workshop topics are:

- Defense in Depth is a Smart Investment
- Trust Anchors are Invulnerable
- Data Dispersion Enhances Data Security
- Abnormal Behavior Detection Finds Malicious Actors

In discussing these topics we will cover a broad spectrum of security architectures: architectures that focus on securing the perimeter, architectures that focus on building out trust from a solid core, and distributed architectures. We will also discuss architectural implications of human behavior.

Brief descriptions of these four topics will be available at the NITRD web page:
http://cybersecurity.nitrd.gov.

The workshops will be held once a month beginning in March 2011. We will be releasing a call for participation in the Federal Register. Those interested in participating will be asked to submit a very brief curriculum vita or resume that indicates their past work in the topic area and a one page paper stating whether they are pro or con the stated topic and outlining their thoughts on the issue. Travel and expenses for selected participants will be reimbursed.